VZCZCXRO3645
RR RUEHCHI
DE RUEHBK #1942/01 0932337
ZNR UUUUU ZZH
R 032337Z APR 07
FM AMEMBASSY BANGKOK
TO RUEHC/SECSTATE WASHDC 6016
INFO RUEHCHI/AMCONSUL CHIANG MAI 3385

UNCLAS SECTION 01 OF 02 BANGKOK 001942

SIPDIS

STATE FOR IIP/G/EAP (EKENEALY); INFO EAP/PD (JDAVIES, DFIRESTEIN)

SIPDIS

E.O. 12958: N/A
TAGS: OIIP KPAO TH
SUBJECT: REQUEST FOR U.S. SPEAKER FOR DVC ON DELINEATION OF LEGAL AUTHORITY FOR CYBER CRIME LAW ENFORCEMENT

¶1. Program Description: A 120 minute-long digital video conference

¶2. Date and Time of Program: APRIL 23, 2007, 9:00-11:00PM EST (APRIL 24, 8:00-10:00AM Bangkok time)

¶3. Background: In January 2007, Thailand's National Legislative Assembly (NLA) approved for consideration a Cyber Crime Bill, which is currently under scrutiny of the Special Committee appointed by the NLA. The main purpose of this review is to amend some legal concepts and to make it much more practical and efficient in taking legal action against cyber crime perpetrators. The Cyber Crime Bill will establish criteria to determine criminal offenses committed by cyber crime perpetrators; establish a special cyber cop agency or entity to enforce this law by giving it more power to compile electronic evidence sent via the Internet and by electronic devices; and empower the State through the Ministry of Information and Communications Technology (MICT) under the court' s review to block or close websites which display content illegal under Thai law, such as pornography, terrorist support, and contempt of the King. Currently there is no law enabling the government to order Internet Service Providers (ISPs) to close websites containing this sort of content. The MICT makes formal requests of Internet service providers to block websites "voluntarily".

The cyber crime law will formalize current blurred lines of cyber crime investigation oversight and cyber crime law enforcement authority among Thai Government bodies. There remains substantial debate among the Thai drafters on how the Thai government should organize itself internally to deal with the investigative, law enforcement, and judicial roles it will be taking on.

The Members of the Special Committee are now studying problems, solutions and experiences of U.S. federal, state, and local authorities in enforcing cyber crime laws in the US, especially during the initial period when the FBI, local police, sheriffs or magistrate courts first started cooperating on these issues. The Special Committee is also interested in learning about U.S. experience in arresting hackers (such as Kevin Mitnick) and about computer forensics data compilation from online service providers (OSPs), Internet service providers (ISPs) and telecom operators, before passing this Bill to the NLA for further promulgation.

This is the second of what will be a three-part DVC series. The first DVC on Internet Censorship and Regulation took place March 15, ¶2007. A speaker request for our third DVC on Computer Forensics will follow SEPTEL.

¶4. Purpose of Program:
a) To explain the interrelationships and legal lines of authority among federal, state, and local law enforcement bodies and the courts, with emphasis on fighting cyber crimes;
b) To be a resource to the Thai cyber crime bill drafting committee in its deliberations over the legal and administrative purview of the proposed Cyber cop authority;
c) To encourage coverage of this issue by Thai media

¶5. Type of Speaker Requested: The drafting committee is looking to the U.S. experience for information on how USG (federal) law enforcement branches like the Departments of Justice and Homeland Security, and state and local law enforcement officials cooperate and work with the courts to bring cyber crime perpetrators to justice. Post seeks a legal expert with both experience in cyber crime prosecution and a law enforcement background who is also very familiar with the administrative and legal authority of federal, state, and local law enforcement officials in the U.S. This person should be knowledgeable about any problems of jurisdiction that have arisen in the establishment of these lines of authority in the U.S., particularly since the establishment of the Department of Homeland Security and passage of the U.S. Patriot Act, and how they were resolved. Some knowledge of Thailand and recent political developments would be useful but not required.

¶6. Anticipated Audiences: Panelists will be members of the cyber crime bill drafting committee; the Minister of Information and Communications Technology, who chairs the drafting committee, will be invited. About 15-20 people in all, including academicians and select members of the local media, are expected to attend. Simultaneous English-Thai translation will be provided.

¶7. Funding: All speaker costs will be covered by Post's program funds.

¶8. Program Contact Information:
a) Program Officer:
Mr. William Flens
Public Diplomacy Officer
Tel: (66-2) 205-4849; Fax: (66-2) 650-8924
Mobile: (66-81) 174-9012
E-mail: Flensw@state.gov

b) Program Assistant
Bussabonglahwan Pattaro
Press Specialist
Tel: (66-2) 205-4418; Fax: (66-2) 650-8919
Mobile: (66-81) 833-1112
E-mail: Pattaro@state.gov

ARVIZU